Spaceflight Project Security: Terrestrial and On-Orbit/Mission

PM Challenge 2007

Randy Seftas and Joshua Krage
NASA Goddard Space Flight Center
Greenbelt, MD

Agenda

- Highlights from:
  - National Space Policy Protection
  - GSFC Space Asset Protection
- Cyber:
  - Attacks, Impacts, and Issues
  - Threat Sources/Adversaries
- Trends

National Space Policy Protection Highlights

2. **Principles**: The United States considers space capabilities -- including the ground and space segments and supporting links -- vital to its national interests. Consistent with this policy, the United States will: …. *take those actions necessary to protect its space capabilities*.

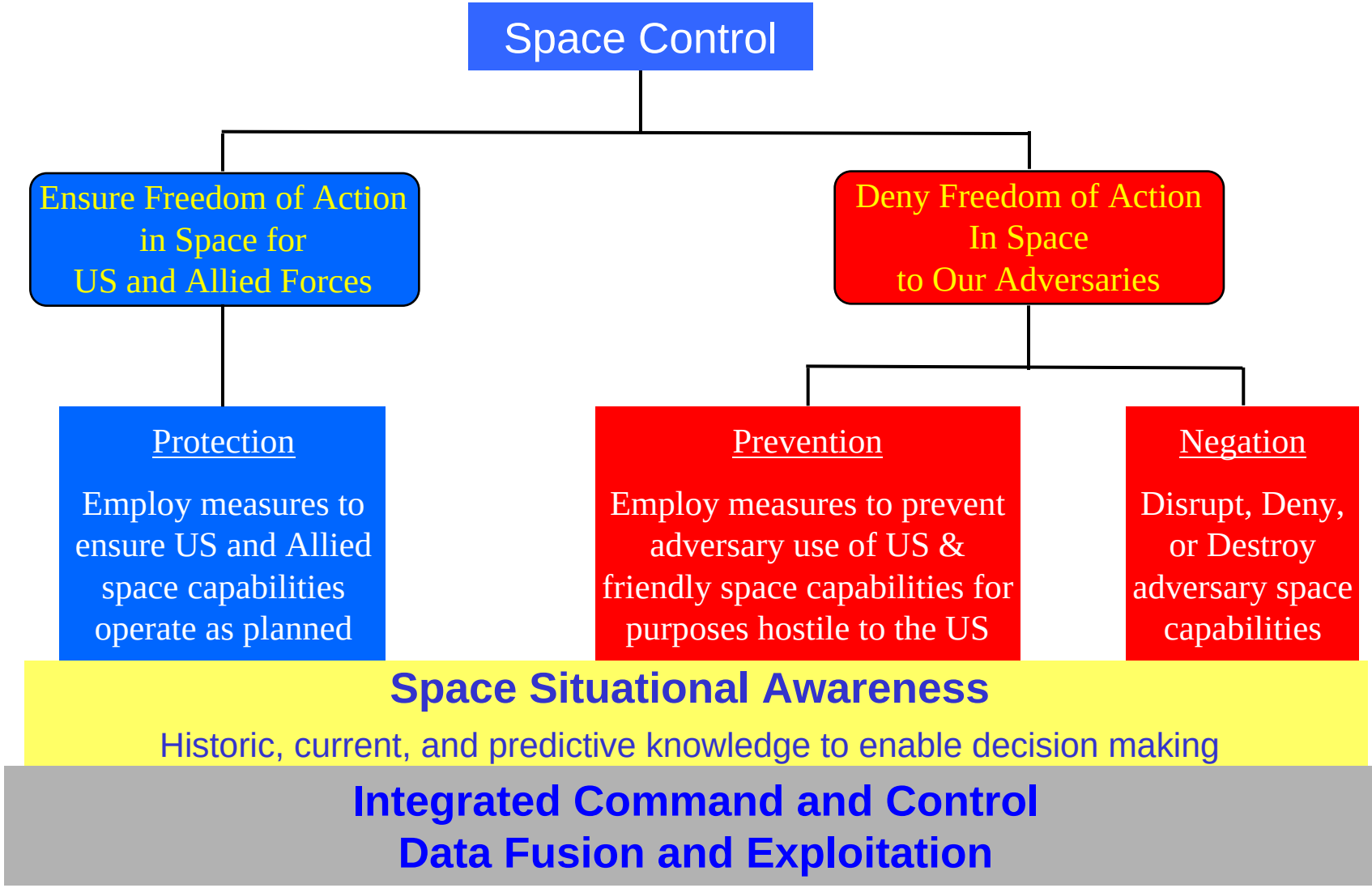
5. **National Security Space Guidelines**: To achieve the goals of this policy, the Secretary of Defense (SECDEF) shall: Have responsibility for space situational awareness; in this capacity, the SECDEF shall support the space situational awareness requirements of the Director of National Intelligence and conduct space situational awareness for: …. *civil space capabilities and operations, particularly human space flight activities*.

National Space Policy Protection Highlights (cont)

11. **<u>Orbital Debris</u>**: Orbital debris poses a risk to continued reliable use of space-based services and operations and to the safety of persons and property in space and on Earth. The United States shall seek to minimize the creation of orbital debris by government and non-government operations in space in order to preserve the space environment for future generations. Toward that end:

- Departments and agencies shall continue to follow the United States Government Orbital Debris Mitigation Standard Practices, consistent with mission requirements and cost effectiveness, in the procurement and operation of spacecraft, launch services, and the operation of tests and experiments in space.

Space Control Objectives and Missions



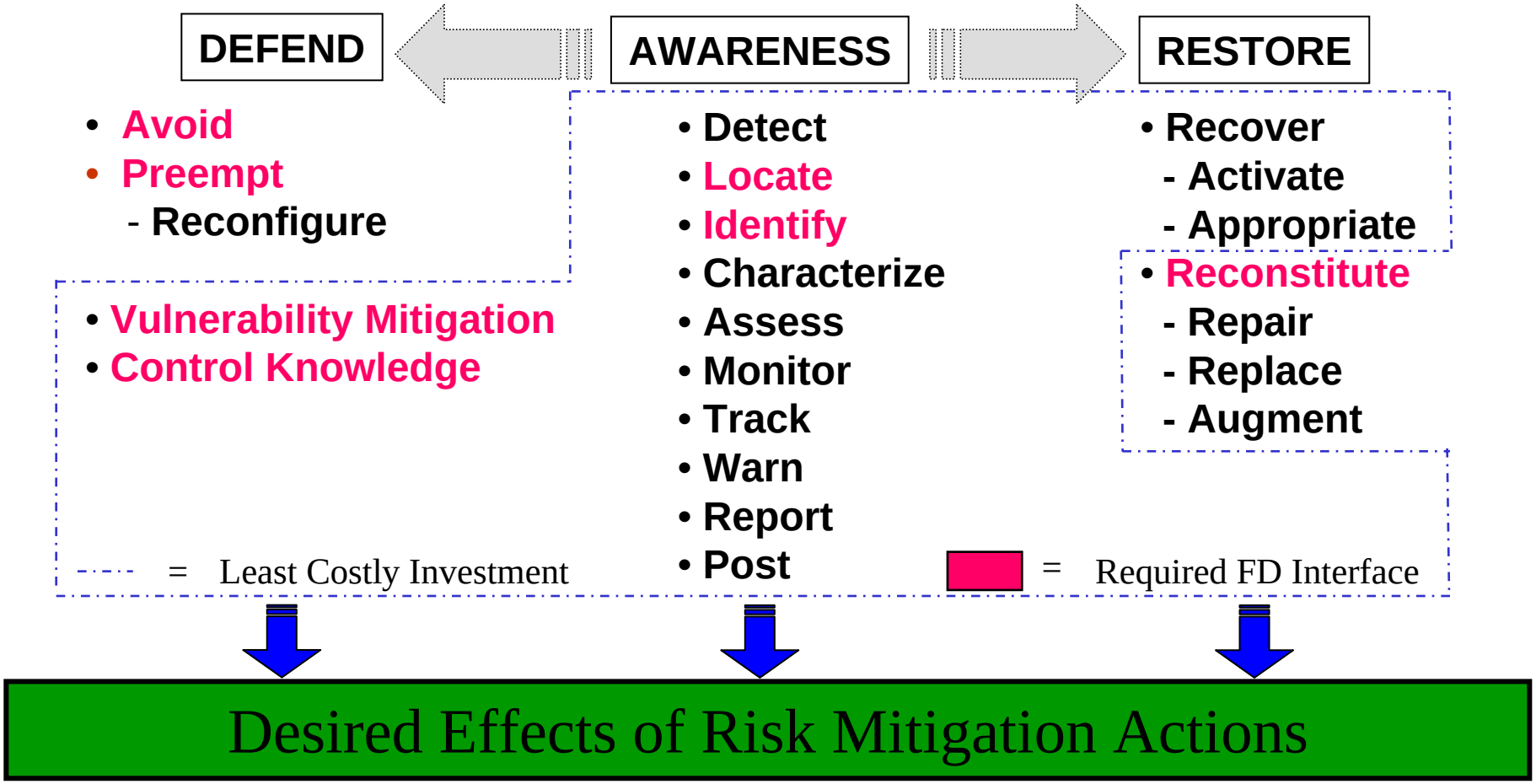
Goddard's Space Asset Protection Highlights

- Space asset protection involves the planning and implementation of measures to protect space assets from intentional or unintentional disruption, exploitation or attack, whether natural or man-made.
- Space asset protection includes aspects of personnel, physical, information, communications, information technology, and operational security.
- Effective protection requires a ***risk management vice risk avoidance*** approach, consistent with existing policies, approved mission requirements, and fiscal realities.
- The Center shall ensure that space asset protection functional support is provided to missions and management, including at a minimum, support in the development of ***threat assessments, identification of risks, and identification of protection strategies appropriate for the threats and risk levels identified***.
- Space asset protection functional support shall be ***led by the Mission Engineering and Systems Analysis Division, Code 590***, with support from the Information Technology and Communications Directorate, Code 700, and other organizations as appropriate.

Goal / Objectives / Approach

- Goal
  - Protect space assets from intentional or unintentional disruption, exploitation or attack, whether natural or man-made
- Objectives
  - Mitigate or eliminate vulnerabilities and single points-of-failure in the infrastructure of space systems
  - Elevate the space situational awareness of managed missions
- Approach
  - Transfer best protection practices from DOD/IC organizations, in particular the NSSO and the NRO.
    - Leverage ongoing DOD/IC Defensive Space Control investments, activities, countermeasures and resources
  - Integrate institutional security capabilities to eliminate single points of failure
  - Focus protection resources to achieve greater space situational awareness (less investment than either “defend” or “restore”)
  - Spin-off DOD/IC DCS countermeasures to support current space flight operations or science data processing activities

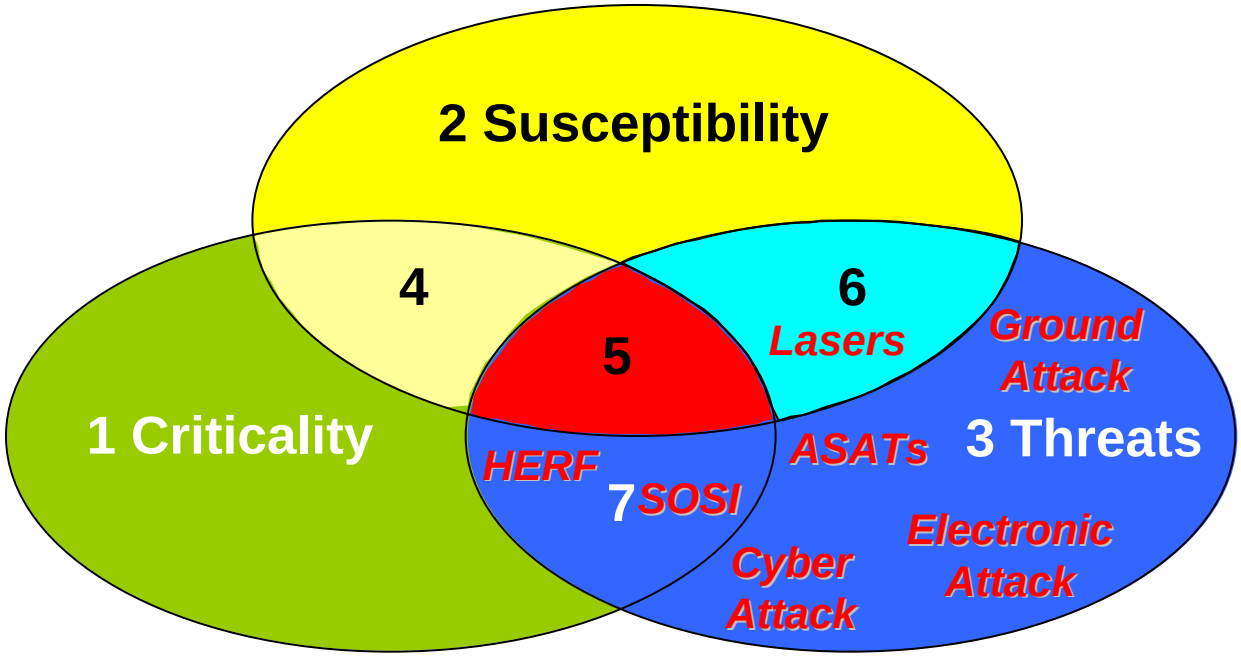
Protection for Space Mission Assurance Functional Construct



Desired Effects of Risk Mitigation Efforts

DEFEND	AWARENESS	RESTORE
Capability survival or endurance**.**	***Sustain our knowledge base and reporting*** of the natural and threat environment, indications of adversary intent and motivation, and of our space capabilities and status.	The ***quick recovery*** from attack.
Prevent, deter and dissuade attacks.	***Maintain vigilance*** over the natural and threat environment and our space capabilities for the purpose of tracking movement and changes to posture and status of attacks, threats, natural hazards and events, and our space assets.	The ***timely reconstitution*** of mission capability
	Be alert to the implications of movement, changes to posture and other indications, and quickly draw inferences about threats, intentions and attacks, or the potential for a natural event or hazard.	
	Monitor status, changes, anomalies and malfunctions in our space capabilities, understand their implications, and quickly determine and attribute the cause.	
	Issue timely warnings of potential or impending attacks or natural events, and direct the appropriate course of action.	

Space Asset Protection Risk Model



1 – Critical assets for which there are no known susceptibilities and no validated threats
2 – Susceptibilities in systems, hardware, software, equipment or facilities which are not associated with critical assets and for which there are no validated threats
3 – Threat environment for which there is no valid threat to critical assets or access to susceptibilities (or susceptibility information)
4 – Critical assets for which there are known susceptibilities but no valid threats
5 – Critical assets for which there are known susceptibilities and valid threats
6 – Valid threat has acquired specific knowledge and/or capability to exploit a susceptibility in an asset however, the asset is not critical
7 – Critical asset for which there are no known susceptibilities but there is exposure to a valid threat

Threat x Susceptibility = Vulnerability

Space Object Surveillance and Identification (SOSI) - Knowledge of a satellite's position and velocity can now be obtained using relatively unsophisticated optical, radar, and signal tracking systems.	Anti-Satellite Weapons (ASATs) - ASATs come in a variety of forms, from missiles tipped with nuclear warheads to low-altitude direct ascent interceptors. These weapons are typically ground or air launched into intercept trajectories or orbits that are nearly the same as the intended target satellite.
Ground Segment Attack or Sabotage - One of the easiest ways to disrupt, deny, degrade, or destroy the utility of a space system is to attack or sabotage its associated ground segment elements.	Lasers - Low-power lasers are typically designed to spoof or jam satellite electro-optical sensors using laser radiation that is in the sensor pass band (in-band), thus temporarily blinding the satellite. High-power lasers can permanently damage or destroy a satellite by radiating enough energy to overheat its parts.
Electronic Attack on Communications, Data and Command Links - Electronic attack is defined as any action involving the use of electromagnetic energy and directed energy to control the electromagnetic spectrum or to attack an adversary.	Radio Frequency ASAT Weapons - RF ASAT weapons concepts include ground- and space-based RF emitters that fire an intense burst of radio energy at a satellite, disabling electronic components.
Cyber Attack - Hacking, whether “for fun” or some other purpose, is clearly a widespread phenomenon with ground-based systems, and NASA is a popular target.	

Evolution of Cyber Attacks

- Early in the space age…
  - Attacking (or just understanding) space assets and support systems required extensive knowledge and physical access
  - It wouldn't be "right" to sabotage the program
  - Only the "space age" nations could play
- Then came PCs, the Internet, and the tech explosion..
  - Access and information are now "just a hop away" on the Internet
    - Geographic barriers and physical access are no longer pre-requisites
    - Easy access to information on building and operating spacecraft
  - Satellite use is so commonplace that amateur satellites are being launched
    - The pool of experienced space operators is now very large
- And now we're beginning the information warfare era
  - Cyber attacks are becoming both commonplace and part of military capabilities, including integrated operations
  - Non-Government organizations can now level the playing field

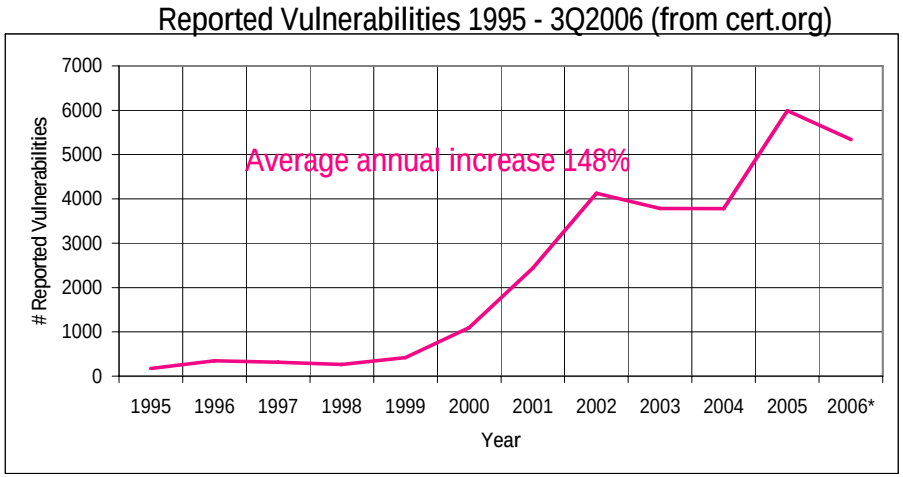
The Potential Cyber Impact

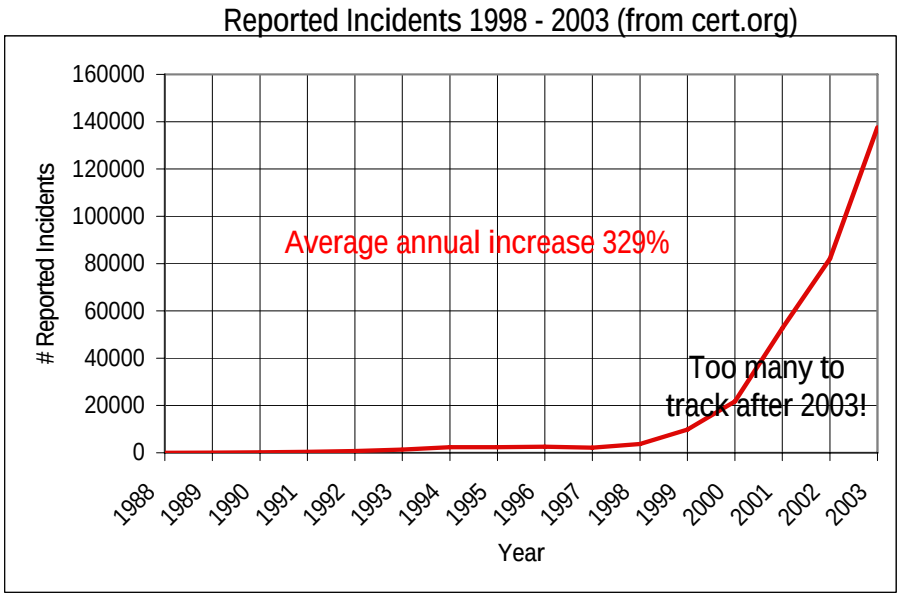
- Several studies have been conducted around the "survivability" of unprotected Internet systems
  - The average time is currently measured in minutes and continues to diminish and new systems on the Internet are probed or attacked within seconds of becoming active
    - Its akin to keeping air contained while in a vacuum -- any unchecked damage can become a breach
  - Attacks are so cheap and easy to launch, they have become omnipresent and impossible to avoid -- *everyone* is being attacked at all times
- The sheer number of different types of attacks poses defensive challenges
  - New vulnerabilities are identified routinely
  - Miss one vulnerability, or be slow in responding, and an attacker can breach the system
  - Internet systems are constantly being breached

Support systems on the Internet can quickly become the project's weakest link

An Explosion of Cyber Issues

- Since the dawn of recorded (Internet) time, cyber vulnerabilities and reported successful incidents have blossomed
  - New vulnerabilities are identified through research, independent validation, and black box testing
  - Incidents are self-reported, which tends to be a lower bound due to concern over reputation and liability
  - Damages from these incidents are quite difficult to calculate, especially when intangible elements such as reputation are considered





Additional Challenges

- Every space asset has associated terrestrial support systems that are increasingly:
  - Challenged to do more with less
  - Dependent on information systems
  - Dependent on external resources
  - Connected to partners at other organizations
  - Complex
  - Remaining operating beyond completion of the mission objectives

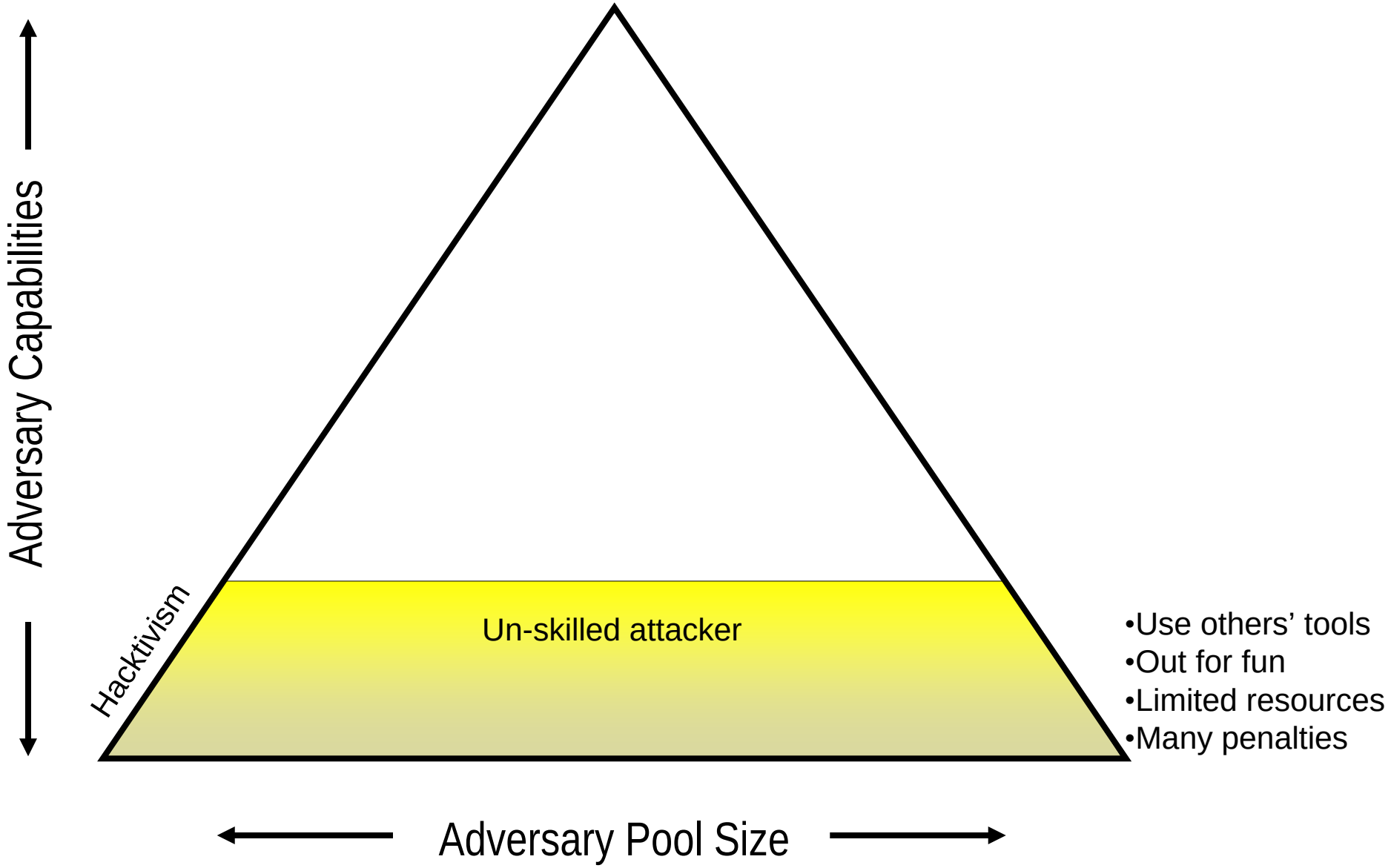
At the same time, adversaries are significantly increasing the knowledge and resources focusing on understanding and exploiting space assets and support systems.

Cyber Threat Sources

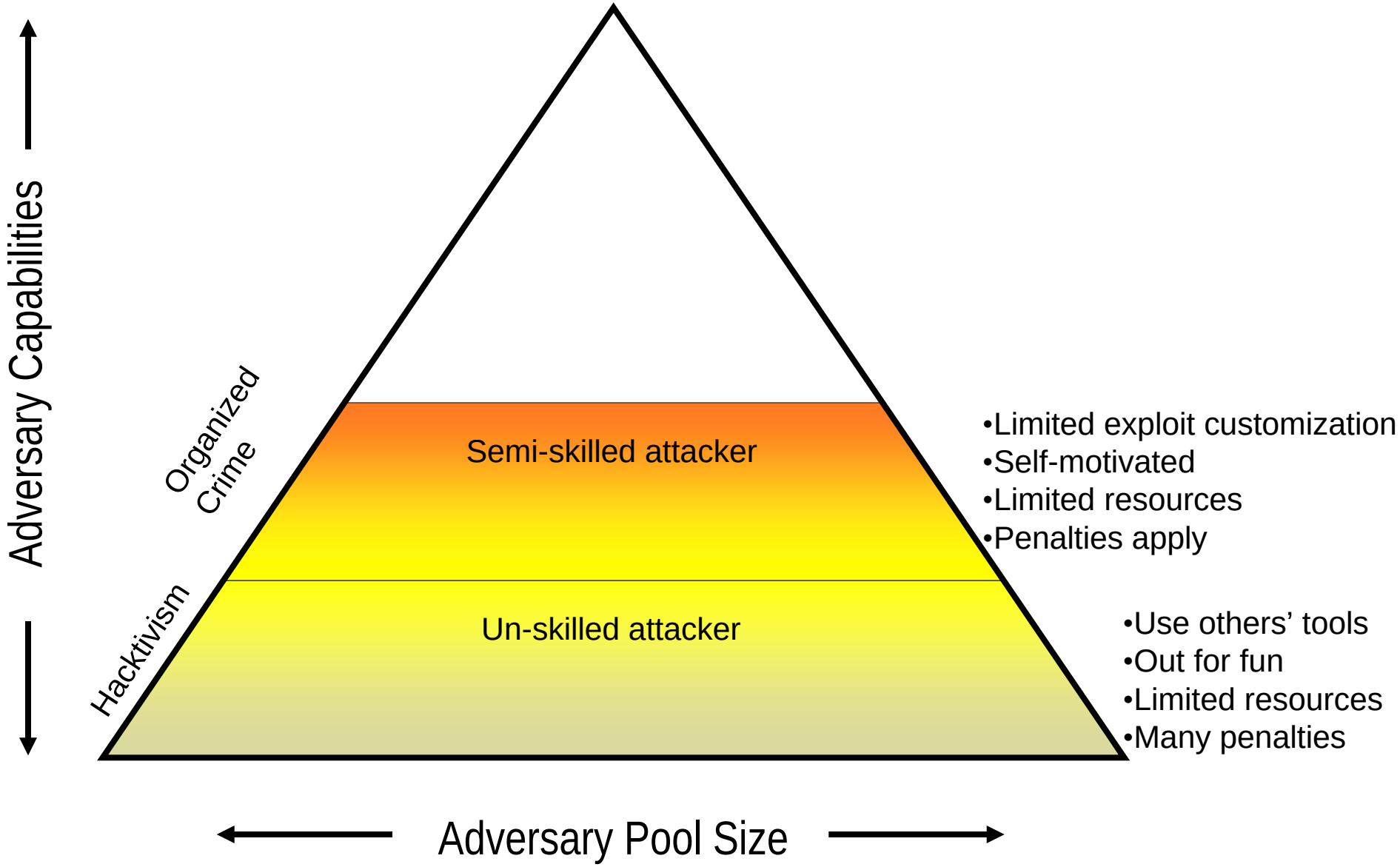
- The most severe threats involve the intelligent adaptive adversary who:
  - Actively works to defeat defenses
  - Will change tactics and tools mid-course
  - Is generally unpredictable
  - Has specific objectives in mind
  - Can attack any vulnerability, while the defender must protect everything
  - Can develop and test new attack methods without the defender's knowledge

The most dangerous adversary is not the most numerous (yet)

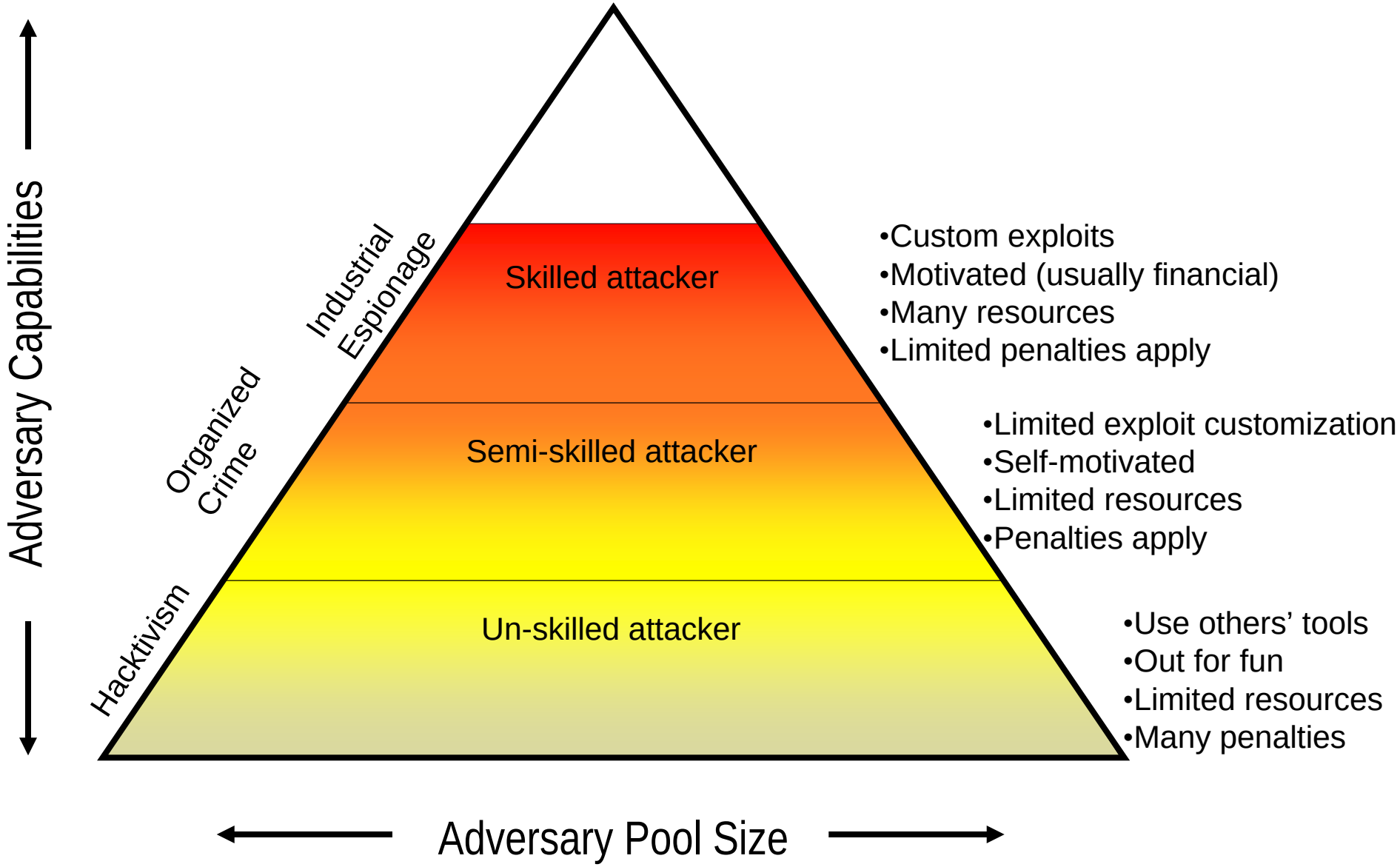
Cyber Adversary Pyramid



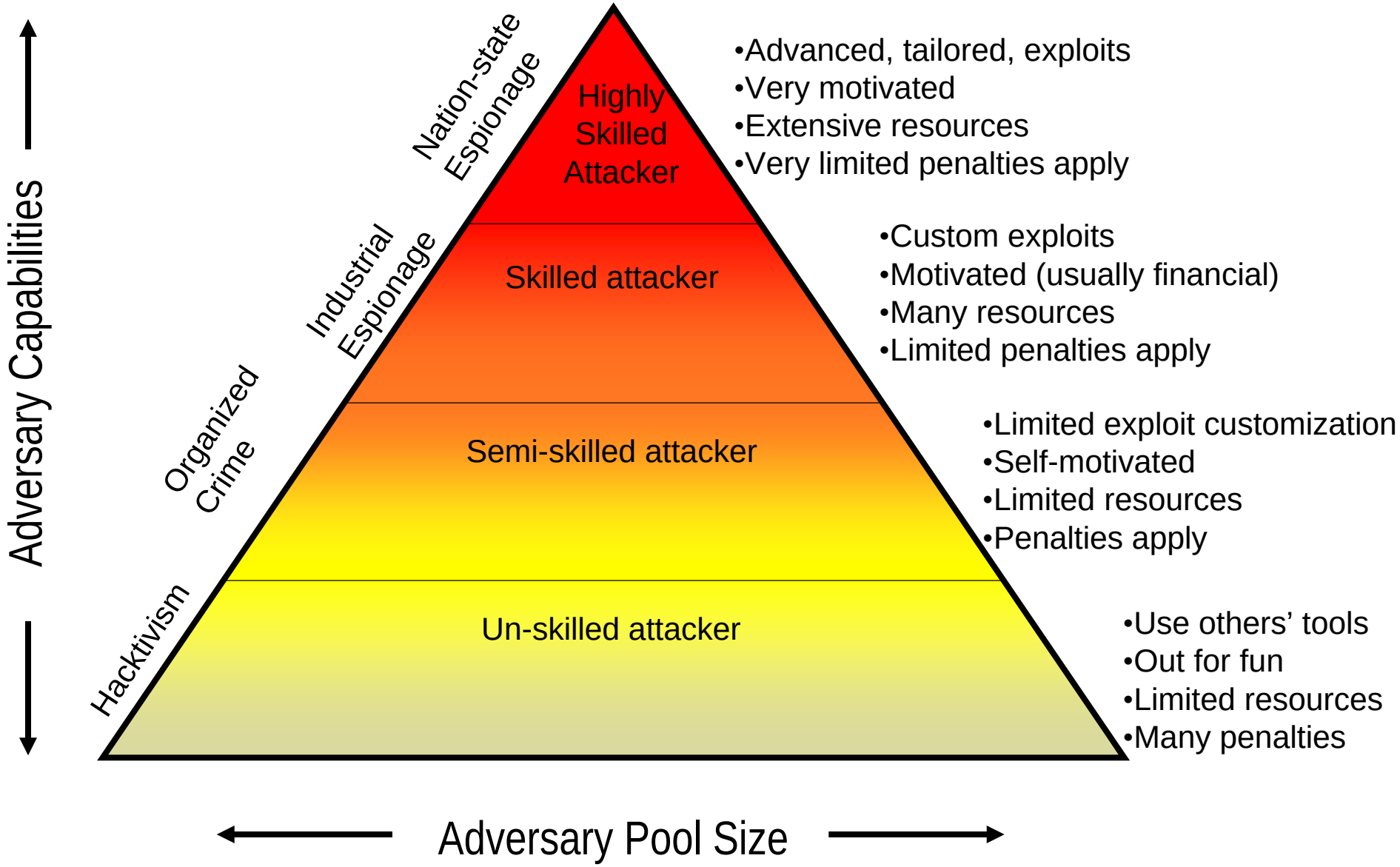
Cyber Adversary Pyramid



Cyber Adversary Pyramid



Cyber Adversary Pyramid



SCADA and Spacecraft Systems Similarities

- Supervisory Control and Data Acquisition (SCADA) systems are a subset of industrial control systems
  - Used in community infrastructure to manage utilities
  - Part of the nationwide critical infrastructure

- SCADA systems are similar to spacecraft systems in that they both…
  - Depend on highly specialized hardware such as embedded systems and realtime operating systems
  - Have operators sensitized to the need to protect integrity and availability of the controlled systems
  - Require dedicated practice and experience to develop the requisite skillset to manage the systems
  - Were not initially designed to be targets of deliberate attacks
  - Are current targets of skilled adversaries

Cyber Trends

- Attackers continue targeting the weakest link: people
  - Design/configuration flaws in hardware and software
  - Individual end-users are being actively targeted, with the attacker convincing the user to take a specific action
  - Simple, common mistakes continues to be the low hanging fruit
- Financial motivation continues to improve
  - Blackmail, competitive “edge”, direct $$ return
- Cyber/Information warfare will continue to develop as a dedicated discipline
  - Groups will continue to develop experience and establish footholds in neutral territory (such as a home user’s computer)
  - More nation states will officially incorporate information warfare capabilities into their military structure
  - The adversary pool size and overall capabilities will improve rapidly
- Complex environments, e.g. space systems, continue to move from black to crystal boxes
  - Attackers continuously increase their knowledge pool

Stemming the Tide

- Cyber countermeasures:
  - Must be tailored to the project and organizational objectives
  - Need to be improved, and evolve, across the board
    - Protect the support systems and operational policies as aggressively as the command and control systems
  - Require active responses within the infrastructure
    - In turn, requires detailed understanding of how it works, what can break, and how any external dependencies can affect you
  - Need to have the ability to make changes in ground and support systems rapidly
    - Long lead times and configuration freezes are becoming issues by creating windows of "risk through lack of change"
  - Require paranoia regarding deliberate man-made actions, both internal and external
    - If it can go wrong, it will
    - If it can *be made to* go wrong, it will

Space Asset Protection Trends

- The nation's defense and economic dependence on space derived information will continue to increase.
- Current trends in technology proliferation, accessibility to space, globalization of space programs and industries, commercialization of space systems and services, and foreign knowledge about U.S. space systems increases the likelihood that vulnerable U.S. space systems will come under attack.
- The ability to restrict or deny freedom of access to and operations in space is no longer limited to global military powers.
- Knowledge of U.S. space systems functions, locations and physical characteristics, as well as the means to conduct counter-space operations is increasingly more available on the international market

Questions?

- Contact information:
  - Randy Seftas Space Asset Protection
    George.R.Seftas@nasa.gov
    +1 301 614 5122
  - Joshua Krage Information Security
    Joshua.Krage@nasa.gov

Backup Slides

Space Situational Awareness Tasks

- **Environmental Information**
  - Monitor, characterize, predict and report on the space related environment, i.e, *terrestrial weather; atmospheric*, *ionospheric*, *magnetospheric*, *solar and interplanetary conditions.*
    - Significant "Push" and "Pull"
- **Orbital and Network Information**
  - Detect, track, identify and catalog man-made objects in space
    - "Push" state vectors for operational missions from LEO out to GEO
    - "Pull" catalog data from archive to support in-house collision avoidance
  - Provide battle-space information and services
    - "Pull" signal/laser de-confliction and space network nodal analysis
- **Event Information**
  - Detect, process and report space events, i.e, *launches*, *orbital maneuvers*, *break-ups*, *reentries*, *orbital decay*, *dockings*, *etc.*
    - "Push" state vectors for operational missions after maneuvering
    - "Pull" catalog data from archive to support in-house collision avoidance

Space Situational Awareness Tasks (cont)

- **Event Information (cont)**
  - Characterize, assess and resolve anomalies/attacks on all space systems, i.e, *provide I&W of attacks, support resolution of anomalies, provide sufficient information to attribute source of attack/interference, etc.*
    - "Push" operational status of missions
    - "Pull" technology (sensors and automation) that supports DOD capabilities for generating event information.
- **US Space System Information**
  - Maintain the status and characteristics of Blue Space Forces/Assets, i.e, *physical properties, current status, vulnerabilities, constellation composition, etc.*
    - "Push" operational status and vulnerabilities of missions
    - "Pull" same/similar bus engineering/operations information to assist in fault isolation and anomaly resolution of spacecraft.

Space Situational Awareness Tasks (cont)

- **Space Intelligence Information**
  - Provide intelligence on foreign and adversary space systems, i.e, *space related communications links, on-orbit asset locations, etc.*
    - "Pull" intelligence information when required to protect missions.
  - Maintain current foreign and adversary space system characteristics and operating parameters, i.e, *physical and signal properties, function, signal internals and operating parameters, etc.*
    - "Pull" intelligence information when required to protect missions.
  - Detect, monitor and report on foreign and adversary terrestrial space systems, i.e, *fixed and mobile systems for command and control, launch and exploitation, etc.*
    - "Pull" intelligence information when required to protect missions.
  - Develop predictive battle-space awareness on adversary strategies, tactics, intent, activity, and knowledge, i.e, *identify adversary centers of gravity, likely courses of action, strengths and vulnerabilities to support targeting and intelligence collection, etc.*
    - "Pull" intelligence information when required to protect missions.

Space Asset Vulnerability References

- China Attempted To Blind U.S. Satellites With Laser
  http://www.defensenews.com/story.php?F=2121111&C=america
- China a Major Cyberthreat, Commission Warns
  http://www.fcw.com/article96975-12-01-06-Web
- Combating Satellite Terrorism, DIY Style
  http://www.popularmechanics.com/technology/military_law/4205155.html
- US Warns of threat to satellites
  http://www.centredaily.com/mld/centredaily/news/16231120.htm
- The Increased Threat to Satellite Communications
  http://satjournal.tcom.ohiou.edu/Issue6/overview2.html
- Hacker Infiltrates Military Satellite [UK, never substantiated]
  http://www.theregister.com/1999/03/01/hacker_infiltrates_military_satellite/
  http://www.interesting-people.org/archives/interesting-people/199902/msg00087.html
- The Great Satellite Caper
  http://www.time.com/time/magazine/article/0,9171,1048422,00.html
- Another Suspected NASA Hacker Indicted
  http://news.zdnet.com/2100-1009_22-6140001.html
- Unpatched PCs Compromised in 20 Minutes
  http://news.com.com/2100-7349_3-5313402.html